



TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

Déclarations en vertu de la règle 4.17 :

- *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour la désignation suivante US*
- *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour la désignation suivante US*
- *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour la désignation suivante US*
- *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : Le procédé permet de vérifier que des données reçues par un récepteur (2) ont été envoyées par un émetteur (1, 3) autorisé par un tiers de confiance, l'émetteur et le récepteur étant raccordés à un réseau numérique. Un identifiant (IdEvent) est associé aux données envoyées par l'émetteur et, lorsque les données sont reçues par le récepteur (2), celui-ci génère un nombre aléatoire (C) qu'il diffuse sur le réseau. L'émetteur qui reçoit ce nombre aléatoire calcule une réponse (R) en appliquant une première fonction (G) au nombre aléatoire (C) et à l'identifiant (IdEvent) et envoie cette réponse (R) au récepteur qui vérifie la réponse reçue en appliquant une seconde fonction (H) à la réponse reçue, au nombre aléatoire (C) et à l'identifiant (IdEvent). La première fonction (G) est délivrée au préalable à l'émetteur par le tiers de confiance et la seconde fonction (H) est une fonction de vérification du résultat de la première fonction, délivrée au préalable par le tiers de confiance au récepteur.

Procédé d'authentification anonyme d'un émetteur de données

Domaine de l'invention

La présente invention concerne l'échange sécurisé de données à
5 travers un réseau reliant différents dispositifs et l'authentification de la source
de données émises sur un réseau.

Etat de la technique

Dans certains cas, il est nécessaire pour un dispositif récepteur de
10 données d'être sûr que l'émetteur qui a diffusé les données était bien autorisé à
le faire par un tiers de confiance sans que le récepteur des données ne
connaisse l'identité de l'émetteur, les données étant également susceptibles
d'être relayées par un dispositif intermédiaire. Or tous les schémas connus
d'authentification d'un émetteur de données impliquent que le récepteur des
15 données connaisse l'émetteur.

Exposé de l'invention

Un but de l'invention est donc de proposer une méthode permettant
à un émetteur de données de prouver qu'il était bien autorisé à émettre les
20 données par un tiers de confiance sans que le récepteur des données ne
connaisse l'identité de l'émetteur.

A cet effet, l'invention concerne un procédé permettant de vérifier
que des données reçues par un récepteur ont été envoyées par un émetteur
autorisé par un tiers de confiance, l'émetteur et le récepteur étant raccordés à
25 un réseau numérique. Selon l'invention, un identifiant est associé aux données
envoyées par l'émetteur et le procédé comprend les étapes consistant, pour le
récepteur, à :

- (a) générer un nombre aléatoire ;
- (b) diffuser sur le réseau ledit nombre aléatoire ;
- 30 (c) recevoir de l'émetteur une réponse calculée en appliquant une
première fonction audit nombre aléatoire et audit identifiant ; et
- (d) vérifier la réponse reçue en appliquant une seconde fonction à la
réponse reçue, audit nombre aléatoire et audit identifiant ;
- la première fonction ayant été au préalable délivrée à l'émetteur par
35 le tiers de confiance et la seconde fonction étant une fonction de vérification du
résultat de la première fonction, délivrée au préalable par le tiers de confiance
au récepteur.

L'émetteur peut être soit l'émetteur initial des données dans le réseau, soit un intermédiaire entre l'émetteur initial et le récepteur des données qui a par exemple stocké les données émises par l'émetteur initial.

Selon une variante de l'invention, l'étape (b) est remplacée par une
5 étape consistant à envoyer le nombre aléatoire à l'émetteur.

Selon un mode de réalisation de l'invention, le récepteur interdit l'accès aux données si la réponse reçue à l'étape (c) n'est pas correcte ou si aucune réponse n'est reçue après l'expiration d'un délai prédéterminé à compter de l'émission du nombre aléatoire.

10 L'identifiant associé aux données envoyées par l'émetteur est préférentiellement un nombre aléatoire généré par l'émetteur initial des données dans le réseau et attaché à ces données par l'émetteur initial. Bien entendu, cet identifiant ne donne aucune information sur l'identité de l'émetteur.

L'invention concerne également un procédé pour prouver que des
15 données envoyées à un récepteur ont été émises par un émetteur autorisé par un tiers de confiance, l'émetteur et le récepteur étant raccordés à un réseau numérique. Selon cet aspect de l'invention, un identifiant est associé aux données envoyées par l'émetteur et le procédé comprend les étapes consistant, pour l'émetteur à :

20 (a) recevoir un nombre aléatoire du récepteur ;
(b) calculer une réponse en appliquant une première fonction audit nombre aléatoire et audit identifiant ;
(c) envoyer la réponse au récepteur.

La réponse est susceptible d'être vérifiée par le récepteur en
25 appliquant une seconde fonction à la réponse reçue, audit nombre aléatoire et audit identifiant ; la première fonction ayant été au préalable délivrée à l'émetteur par le tiers de confiance et la seconde fonction étant une fonction de vérification du résultat de la première fonction, délivrée au préalable par le tiers de confiance au récepteur.

30 Selon le principe de l'invention, un tiers de confiance délivre à tous les dispositifs susceptibles d'être des émetteurs initiaux ou intermédiaires dans un réseau, la première fonction permettant de calculer la réponse dans le cadre du procédé ci-dessus. Le tiers de confiance délivre également à tous les dispositifs susceptibles d'être des récepteurs dans le réseau, la seconde
35 fonction permettant de vérifier la réponse calculée à l'aide de la première fonction.

Brève description des dessins

L'invention sera mieux comprise à la lecture de la description qui va suivre, donnée uniquement à titre d'exemple et faite en se référant aux dessins annexés sur lesquels :

- 5 - la figure 1 représente un réseau numérique domestique dans lequel est mise en œuvre l'invention ;
 - les figures 2 et 3 illustrent deux exemples de mises en œuvre de l'invention.

10 Description détaillée de modes de réalisation de l'invention

Sur la base du principe de l'invention exposé ci-dessus, plusieurs scénarios sont possibles.

Selon un premier scénario, un premier émetteur, que nous appellerons Alice, et un second émetteur, que nous appellerons Charlie,
15 diffusent des messages respectivement appelés M_A et M_C sur un réseau auquel est raccordé un récepteur, que nous appellerons Bob. Alice diffuse avec le message M_A un identifiant $IdEvent_A$ qui identifie le message M_A et Charlie diffuse avec le message M_C un identifiant $IdEvent_C$ qui identifie le message M_C .

Alice et Charlie qui sont tous deux raccordés au réseau reçoivent
20 respectivement les messages M_C et M_A émis par l'autre émetteur du réseau mais ils ne les conservent pas. Bob reçoit également les deux messages et nous supposons qu'il ne souhaite conserver que le message M_A . Pour être sûr que M_A provient d'une source autorisée par un tiers de confiance, Bob lance un protocole challenge/réponse de la manière suivante. Bob génère un nombre
25 aléatoire C (le challenge) puis il le diffuse sur le réseau. Alice et Charlie reçoivent tous deux le challenge C .

Au préalable, nous supposons que le tiers de confiance a délivré à Alice et Charlie une fonction G de calcul de réponse et a délivré à Bob une
30 fonction H correspondante de vérification de réponse telle que cette fonction H retourne 0 si la réponse est incorrecte et 1 si la réponse est correcte.

Lorsque Alice et Charlie reçoivent le challenge C émis par Bob, ils calculent respectivement des réponses R_A et R_C comme suit :

Alice : $R_A = G(IdEvent_A, C)$;

Charlie : $R_C = G(IdEvent_C, C)$;

35 puis ils envoient respectivement les réponses R_A et R_C à Bob.

Bob vérifie ensuite chaque réponse en calculant $H(C, R_X, IdEvent_X)$ pour $X = A$ et C . Si tous les résultats retournés par la fonction H sont nuls, alors

Bob ne conserve pas le message M_A qui est considéré comme ne provenant pas d'une source sûre. Par contre, si au moins un résultat retourné par H est égal à 1 (dans l'exemple, il s'agira de $H(C, R_A, \text{IdEvent}_A)$), alors Bob accepte le message M_A car il est assuré qu'il provient d'un émetteur autorisé par le tiers de confiance.

Selon un second scénario, un émetteur, Alice, diffuse un message M_A accompagné d'un identifiant IdEvent_A sur un réseau auquel est raccordé un récepteur Bob et une entité intermédiaire, que nous appellerons Déborah. Dans un premier temps, nous supposons que Bob n'est pas intéressé par le message M_A et qu'il ne le conserve pas. Déborah par contre enregistre le message M_A et son identifiant IdEvent_A .

Plus tard, alors qu'Alice ne diffuse plus de message, nous supposons que Déborah diffuse le message M_A enregistré et son identifiant IdEvent_A sur le réseau. Alice étant seulement un émetteur ne conserve pas M_A . Bob reçoit M_A et souhaite le conserver. Pour s'assurer qu'il provient d'une source autorisée par un tiers de confiance, Bob lance un protocole challenge/réponse de la manière suivante. Bob génère un nombre aléatoire C (le challenge) puis il le diffuse sur le réseau.

Au préalable, nous supposons que le tiers de confiance a délivré à Alice et Déborah une fonction G de calcul de réponse et a délivré à Bob une fonction H correspondante de vérification de réponse telle que cette fonction H retourne 0 si la réponse est incorrecte et 1 si la réponse est correcte.

Alice et Déborah reçoivent le challenge C . Comme Alice n'est pas en train de diffuser un message, elle ne tient pas compte du challenge C . Déborah par contre calcule une réponse $R_D = G(\text{IdEvent}_A, C)$ et envoie cette réponse à Bob. Bob vérifie ensuite cette réponse en calculant $H(C, R_D, \text{IdEvent}_A)$. Si la fonction H retourne 0, alors Bob ne conserve pas le message M_A . En revanche, si la fonction H retourne 1, alors Bob accepte le message M_A qui est considéré comme provenant d'une source autorisée.

On notera que dans les deux scénarios exposés ci-dessus, l'entité récepteur Bob, même s'il est capable de répondre à la source du message, ne sait pas si le message qu'il reçoit provient d'un émetteur (comme Alice) ou d'un intermédiaire (comme Déborah) et surtout il ne connaît pas l'identité du diffuseur du message M_A .

Nous allons maintenant décrire un exemple plus concret de mise en œuvre de l'invention en référence à la figure 1 où sont représentés un décodeur STB (de l'anglais « Set Top Box ») 1, un récepteur de télévision numérique DTV (de l'anglais « Digital Television ») 2 et un dispositif d'enregistrement SU (de l'anglais « Storage Unit ») 3.

Nous supposons que les données diffusées sur ce réseau représentent des programmes audiovisuels composés de flux élémentaires Audio et Vidéo transportés dans un flux de transport de données tel que défini dans la norme ISO/IEC 13818-1 « *Information technology – Generic coding of moving pictures and associated audio information : Systems* ».

Le décodeur 1 représente un émetteur de données sur le réseau, il émet des données qu'il reçoit par exemple d'une antenne satellite ou d'une connexion au câble. Le téléviseur numérique 2 représente un récepteur de données sur le réseau. Le dispositif d'enregistrement 3 représente quant à lui un dispositif intermédiaire capable de rediffuser sur le réseau des données reçues d'un autre dispositif émetteur du réseau.

Ces trois dispositifs sont raccordés à un bus numérique 4, par exemple un bus selon la norme IEEE 1394, et forment ainsi un réseau domestique numérique. Les messages diffusés dans le réseau sont envoyés à travers le canal isochrone du bus 4 et les messages qui sont adressés sont envoyés à travers le canal asynchrone du bus 4.

Le tiers de confiance qui délivre une fonction G de calcul de réponse à un protocole challenge/réponse aux dispositifs émetteurs ou intermédiaires du réseau (dans notre exemple, le décodeur 1 et le dispositif d'enregistrement 3) et qui délivre une fonction H de vérification de réponse aux dispositifs récepteurs du réseau (dans notre exemple le téléviseur numérique 2) est par exemple le fabricant des dispositifs.

En ce qui concerne le choix des fonctions G et H, nous envisagerons trois modes de réalisation.

Selon un premier mode de réalisation préféré, la fonction G est une fonction publique qui utilise une clé secrète K pour calculer une réponse R à partir d'un challenge C et d'un identifiant IdEvent (i.e. $R = G_K(C, IdEvent)$). Pour garantir que les dispositifs émetteurs ou intermédiaires sont des appareils conformes, autorisés par le tiers de confiance, le secret K est inséré dans ces dispositifs, dans une zone de stockage sécurisée qui ne doit plus être accessible ultérieurement (par exemple dans un processeur sécurisé, notamment inclus dans une carte à puce).

La fonction H est dans ce cas une fonction qui calcule une réponse R' à partir du challenge C et de l'identifiant IdEvent en appliquant la fonction G avec la clé secrète K et qui compare ensuite le résultat R' avec la réponse R reçue. H est une fonction booléenne qui délivre une valeur nulle « 0 » si R' est différent de R et qui délivre une valeur « 1 » si R' est égal à R. Dans ce cas, la clé secrète K doit aussi être insérée au préalable par le tiers de confiance dans les dispositifs récepteurs.

Une fonction G correspondant à la définition ci-dessus peut être notamment une fonction de chiffrement telle que la fonction AES décrite notamment dans « *FIPS 197: Specification of the Advanced Encryption Standard (AES)* –26 novembre 2001 » disponible à l'adresse Internet suivante : <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>. Il peut également s'agir d'une fonction de hachage telle que la fonction HMAC-SHA1 décrite notamment dans « *FIPS Publication 198: The Keyed-Hash Message Authentication Code (HMAC)*, National Institute of Standards and Technology, 2001 » disponible à l'adresse Internet suivante : <http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf>.

Dans un second mode de réalisation, la fonction G est une fonction secrète qui est insérée dans les dispositifs émetteurs ou intermédiaires considérés comme conformes et autorisés par le tiers de confiance. Préférentiellement, cette fonction doit être choisie de manière à être très difficilement retrouvée par l'analyse des produits qui la contiennent. De plus cette fonction doit être résistante aux attaques adaptatives à texte clair choisi (plus connues sous le nom anglais de « adaptive chosen-plaintext attacks »).

De même que dans le premier mode de réalisation, la fonction H est dans ce cas une fonction booléenne qui calcule une réponse R' à partir du challenge C et de l'identifiant IdEvent en appliquant la fonction G secrète et qui compare ensuite le résultat R' avec la réponse R reçue, délivrant une valeur nulle « 0 » si R' est différent de R et délivrant une valeur « 1 » si R' est égal à R. Dans ce mode de réalisation, la fonction secrète G doit donc aussi être insérée au préalable par le tiers de confiance dans les dispositifs récepteurs.

Dans un troisième mode de réalisation, les fonctions G et H sont des fonctions publiques utilisant une paire de clés asymétrique (clé privée/clé publique). La fonction G est par exemple une fonction de génération de signature à l'aide d'une clé privée et la fonction H est une fonction de vérification de signature à l'aide de la clé publique correspondante.

Nous utiliserons par exemple les fonctions de signature RSA (acronyme du nom des créateurs Rivest, Shamir et Adleman) comme suit :

$R = G(C, IdEvent) = RSASign_{KPRI}(C, IdEvent)$ et

$H(C, R, IdEvent) = RSAVerif_{KPUB}(C, R, IdEvent)$; où KPRI et KPUB

5 sont la clé privée et la clé publique d'une même paire de clé RSA.

Dans ce cas, la clé privée est insérée dans les dispositifs émetteurs ou intermédiaires du réseau par le tiers de confiance et la clé publique est insérée dans les dispositifs récepteurs du réseau.

10 Nous supposons dans la suite que le premier mode de réalisation a été choisi dans lequel la fonction G est la fonction HMAC-SHA1 et qu'une clé secrète K est incluse dans une zone de stockage inviolable du décodeur STB 1, du récepteur de télévision numérique DTV 2 et du dispositif d'enregistrement SU 3.

15

Premier scénario : le STB transmet directement un programme au DTV

20 Comme illustré à la figure 2, lorsque l'utilisateur du décodeur STB 1 sélectionne un nouveau programme pour qu'il soit diffusé dans le réseau, le STB génère aléatoirement un identifiant de programme IdEvent (étape 20), qui est préférentiellement un nombre de 128 bits et il insère cet identifiant dans des messages contenus dans les paquets de transport des données représentant le programme. Le flux de transport de données est ensuite diffusé sur le réseau
25 (sur le canal isochrone du bus 4) lors de l'étape 21. Il est reçu par le téléviseur numérique DTV 2 qui extrait des paquets de données reçus les messages contenant l'identifiant pour finalement récupérer cet identifiant IdEvent (étape 22).

30 Le DTV génère alors à l'étape 23 un challenge C, qui est préférentiellement un nombre aléatoire de 128 bits, et il diffuse ce challenge C sur le réseau lors de l'étape 24. Lorsque le STB reçoit le challenge C, il calcule à l'étape 25 la réponse :

$R = G(C, IdEvent)$, ou plus précisément :

$R_{STB} = HMAC-SHA1_K(C, IdEvent)$

35 et adresse cette réponse au DTV par le canal asynchrone du bus 4 (étape 26).

Le dispositif d'enregistrement SU 3, qui reçoit également le challenge C ne répond pas puisqu'il n'est pas en train de diffuser des données.

Lorsque le DTV reçoit la réponse $R=R_{STB}$ du STB, il applique la fonction $H(R, C, IdEvent)$ pour vérifier la réponse R (étape 27), ce qui revient à calculer :

5 $R_{DTV} = HMAC-SHA1_K(C, IdEvent)$ et à comparer ce résultat à la réponse R_{STB} reçue. Si les deux valeurs sont les mêmes, alors le DTV considère que le programme reçu provient d'un émetteur autorisé par le tiers de confiance et peut être présenté à l'utilisateur. Sinon, le DTV n'affiche pas à l'utilisateur le programme reçu. Si le DTV ne reçoit aucune réponse après qu'un
10 délai prédéterminé se soit écoulé depuis l'envoi du challenge C sur le réseau, il bloque également l'affichage du programme reçu.

A la fin du protocole, le challenge C et l'identifiant $IdEvent$ sont effacés des mémoires du STB et du DTV.

Second scénario : le STB transmet un programme qui est stocké par
15 le SU qui le diffuse ultérieurement au DTV.

Ce scénario est illustré par la figure 3.

Dans un premier temps, on suppose que l'utilisateur du STB sélectionne un nouveau programme. Le STB génère alors un identifiant $IdEvent$
20 (étape 30) comme dans le premier scénario ci-dessus et il insère cet identifiant dans des messages inclus dans les paquets de transport des données représentant le programme avant de diffuser le flux de transport de données sur le réseau (étape 31).

Le SU enregistre ensuite le flux de données représentant le
25 programme. L'utilisateur a par exemple choisi de ne pas visualiser tout de suite le programme qui est diffusé par le décodeur et préfère l'enregistrer pour le relire plus tard.

Dans un deuxième temps, l'utilisateur souhaite relire le programme enregistré. Le SU diffuse donc le programme sur le réseau lors d'une étape 32.
30 Le DTV reçoit les paquets de données et en extrait les messages contenant l'identifiant $IdEvent$ à l'étape 33.

Le DTV génère ensuite un challenge C comme dans le premier scénario (étape 34) et il diffuse ce challenge sur le réseau (étapes 35, 35').

Le SU reçoit ce challenge C , il calcule donc à l'étape 36 la réponse :

35 $R = G(C, IdEvent)$, ou plus précisément :

$R_{SU} = HMAC-SHA1_K(C, IdEvent)$

et adresse cette réponse au DTV par le canal asynchrone du bus 4 (étape 37).

Le STB qui n'est pas en train de diffuser des données ne répond pas au challenge C qu'il reçoit également.

Lorsque le DTV reçoit la réponse $R=R_{SU}$ du SU, il applique la fonction $H(R, C, IdEvent)$ pour vérifier la réponse R (étape 38), ce qui revient à

5 calculer :

$R_{DTV} = HMAC-SHA1_K(C, IdEvent)$ et à comparer ce résultat à la réponse R_{SU} reçue. Si les deux valeurs sont les mêmes, alors le DTV considère que le programme reçu provient d'un émetteur autorisé par le tiers de confiance et peut être présenté à l'utilisateur. Dans le cas contraire ou dans le cas où

10 aucune réponse n'a été reçue après un délai prédéterminé suivant l'envoi du challenge C par le DTV, ce dernier n'affiche pas à l'utilisateur le programme reçu.

On notera que lorsque le STB a terminé de diffuser le programme dans le premier temps, il efface ensuite l'identifiant $IdEvent$ de sa mémoire.

15 A la fin du protocole, le challenge C et l'identifiant $IdEvent$ sont également effacés des mémoires du SU et du DTV.

Dans une variante de réalisation de l'invention, notamment dans les deux scénarii exposés ci-dessus, il est possible de remplacer l'étape de

20 diffusion sur le réseau du challenge C calculé par le DTV par une étape d'envoi de ce challenge C à l'émetteur des données (le STB dans le premier scénario ou le SU dans le deuxième scénario). Dans ce cas, seul l'émetteur des données reçoit le challenge C. En effet, les protocoles existants de gestion des réseaux numériques permettent à un récepteur de données de répondre à la

25 source des données sans pour autant connaître son identité.

Dans une autre variante de réalisation, le récepteur des données diffuse sur le réseau, en plus du challenge C, l'identifiant $IdEvent$ associé aux données qu'il a reçu (par exemple à l'étape 24 dans la figure 2 ou à l'étape 35,

30 35' dans la figure 3). Chaque appareil émetteur du réseau qui reçoit le challenge C et l'identifiant $IdEvent$ vérifie s'il doit répondre à ce challenge en comparant l'identifiant $IdEvent$ reçu avec celui qu'il vient éventuellement de générer pour diffuser des données. L'émetteur ne répond que si l'identifiant reçu avec le challenge correspond à son identifiant $IdEvent$ courant. Ceci

35 permet d'éviter que tous les émetteurs qui diffusent des données dans le réseau ne répondent lorsqu'un challenge C est envoyé par un récepteur.

L'invention présente notamment les avantages suivants :

Même si plusieurs dispositifs émetteurs ou intermédiaires sont raccordés au réseau, seul celui qui a été autorisé par le tiers de confiance et qui a émis les données est capable de répondre au protocole challenge/réponse initié par le récepteur des données.

5 Le protocole ne divulgue aucune information concernant l'émetteur au récepteur. Ceci permet d'atteindre l'objectif d'une authentification anonyme du dispositif émetteur.

Le protocole repose uniquement sur la couche application et ne requiert aucune particularité au niveau de la couche transport des données.

REVENDICATIONS

1. Procédé pour vérifier que des données reçues par un récepteur
5 (2) ont été envoyées par un émetteur (1, 3) autorisé par un tiers de confiance, l'émetteur et le récepteur étant raccordés à un réseau numérique, caractérisé en ce qu'un identifiant (IdEvent) est associé aux données envoyées par l'émetteur et en ce que le procédé comprend les étapes consistant, pour le récepteur (2), à :
- 10 (a) générer un nombre aléatoire (C) ;
(b) diffuser sur le réseau ledit nombre aléatoire ;
(c) recevoir de l'émetteur une réponse (R) calculée en appliquant une première fonction (G) audit nombre aléatoire (C) et audit identifiant (IdEvent) ;
- 15 (d) vérifier la réponse (R) reçue en appliquant une seconde fonction (H) à la réponse reçue (R), audit nombre aléatoire (C) et audit identifiant (IdEvent) ;
- la première fonction (G) ayant été au préalable délivrée à l'émetteur par le tiers de confiance et la seconde fonction (H) étant une fonction de
20 vérification du résultat de la première fonction, délivrée au préalable par le tiers de confiance au récepteur.
2. Procédé selon la revendication 1, dans lequel l'étape (b) est
25 remplacée par une étape consistant à envoyer ledit nombre aléatoire (C) à l'émetteur.
3. Procédé selon la revendication 1, dans lequel le récepteur diffuse en outre à l'étape (b) ledit identifiant (IdEvent).
- 30 4. Procédé selon l'une des revendications 1 à 3, caractérisé en ce que le récepteur interdit l'accès aux dites données si la réponse (R) reçue à l'étape (c) n'est pas correcte ou si aucune réponse n'est reçue après l'expiration d'un délai prédéterminé à compter de l'émission du nombre aléatoire (C).
- 35 5. Procédé pour prouver que des données envoyées à un récepteur (2) ont été émises par un émetteur (1, 3) autorisé par un tiers de confiance, l'émetteur et le récepteur étant raccordés à un réseau numérique, caractérisé en ce qu'un identifiant (IdEvent) est associé aux données envoyées par

l'émetteur et en ce que le procédé comprend les étapes consistant, pour l'émetteur (1, 3) à :

(a) recevoir un nombre aléatoire (C) du récepteur (2) ;

(b) calculer une réponse (R) en appliquant une première fonction (G)

5 audit nombre aléatoire (C) et audit identifiant (IdEvent) ;

(c) envoyer ladite réponse (R) au récepteur (2) ;

ladite réponse étant susceptible d'être vérifiée par le récepteur en appliquant une seconde fonction (H) à la réponse (R) reçue, audit nombre aléatoire (C) et audit identifiant (IdEvent) ;

10 la première fonction (G) ayant été au préalable délivrée à l'émetteur par le tiers de confiance et la seconde fonction (H) étant une fonction de vérification du résultat de la première fonction, délivrée au préalable par le tiers de confiance au récepteur.

15 6. Procédé selon la revendication 5, dans lequel l'émetteur reçoit en outre à l'étape (a) ledit identifiant (IdEvent) associé aux données reçues par le récepteur et dans lequel les étapes (b) et (c) ne sont effectuées que si ledit identifiant reçu à l'étape (a) correspond à l'identifiant associé aux données que l'émetteur vient d'envoyer.

20 7. Procédé selon l'une des revendications précédentes, caractérisé en ce que l'identifiant associé aux données envoyées par l'émetteur est un nombre aléatoire généré par l'émetteur initial des données dans le réseau et attaché aux dites données par l'émetteur initial.

25 8. Procédé selon l'une des revendications précédentes, caractérisé en ce que la première fonction (G) est une fonction publique utilisant une clé secrète.

30 9. Procédé selon la revendication 8, caractérisé en ce que la seconde fonction (H) est une fonction booléenne

calculant une réponse attendue en appliquant audit nombre aléatoire (C) et audit identifiant (IdEvent) la première fonction (G) avec la clé secrète et comparant la réponse attendue à la réponse reçue pour délivrer :

35 - une valeur « 0 » si les réponses attendue et reçue sont différentes et

- une valeur « 1 » si les réponses attendue et reçue sont égales.

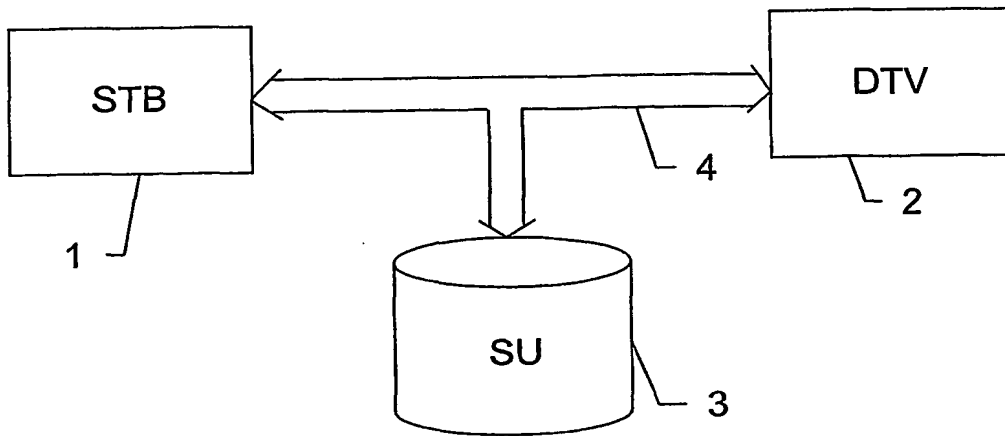
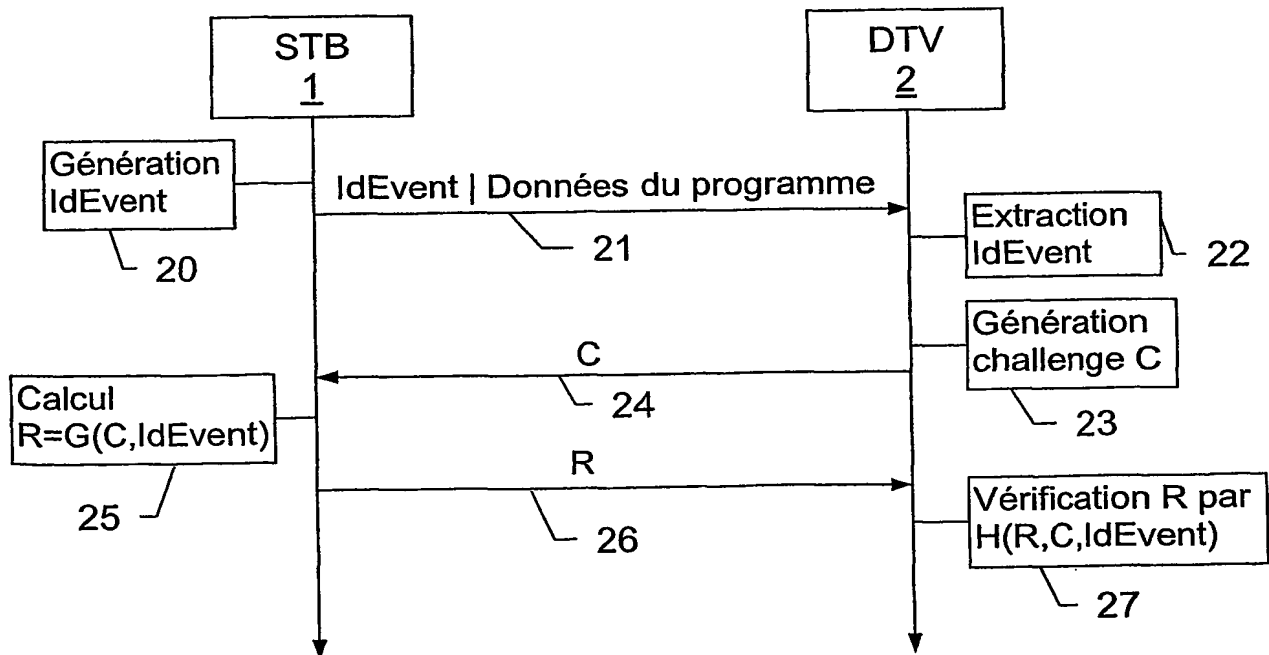
10. Procédé selon l'une des revendications 1 à 7, caractérisé en ce que la première fonction (G) est une fonction secrète.

- 5 11. Procédé selon la revendication 10, caractérisé en ce que la seconde fonction (H) est une fonction booléenne calculant une réponse attendue en appliquant audit nombre aléatoire (C) et audit identifiant (IdEvent) la première fonction (G) et comparant la réponse attendue à la réponse reçue pour délivrer :
- 10 - une valeur « 0 » si les réponses attendue et reçue sont différentes et
- une valeur « 1 » si les réponses attendue et reçue sont égales.

- 15 12. Procédé selon l'une des revendications 1 à 7, caractérisé en ce que la première fonction (G) est une fonction publique de génération de signature à l'aide d'une clé privée.

- 20 13. Procédé selon la revendication 12, caractérisé en ce que la seconde fonction (H) est une fonction publique de vérification de signature à l'aide d'une clé publique correspondant à la clé privée utilisée par la première fonction.

1 / 2

Fig. 1Fig. 2

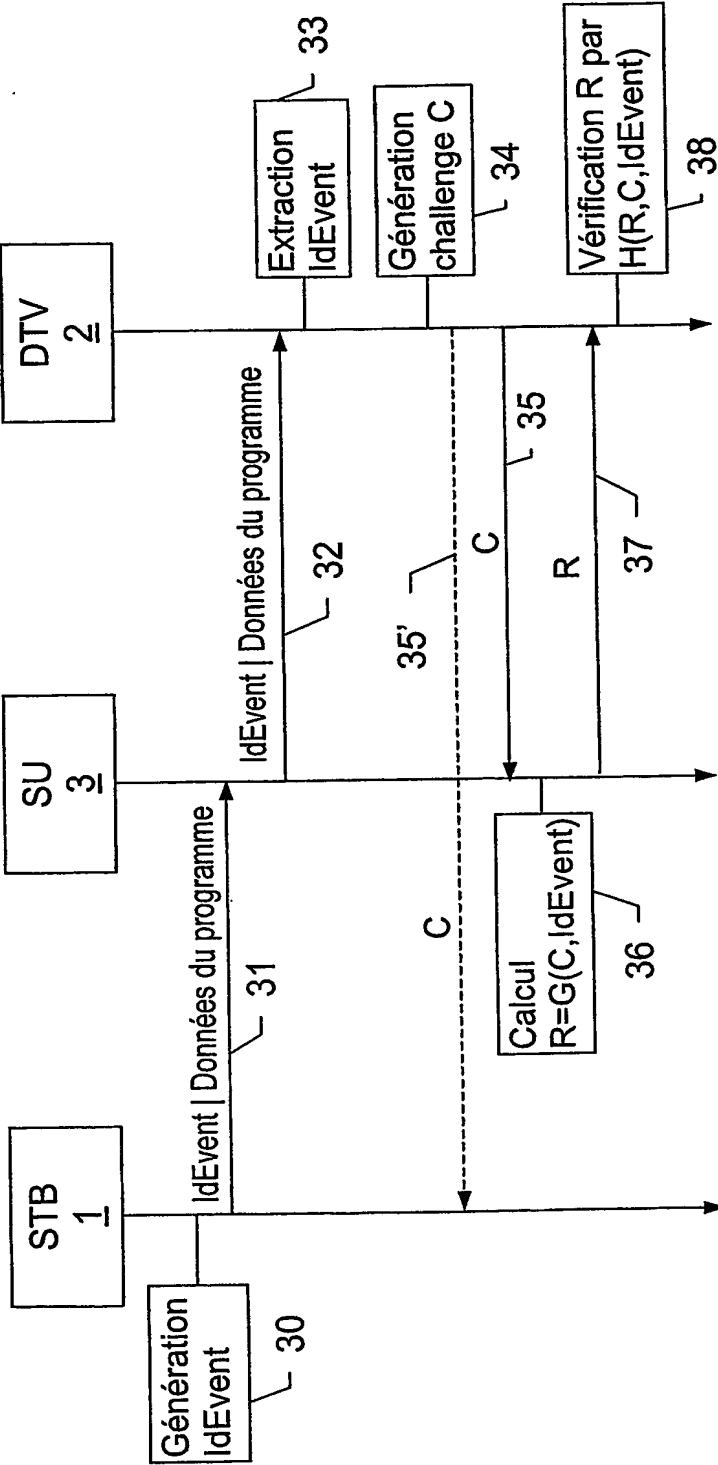


Fig. 3

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international(43) Date de la publication internationale
23 octobre 2003 (23.10.2003)

PCT

(10) Numéro de publication internationale
WO 2003/088612 A3(51) Classification internationale des brevets⁷ :**H04L 29/06, 9/32**(71) Déposant (pour tous les États désignés sauf US) : THOM-
SON LICENSING S.A. [FR/FR]; 46, quai Alphonse Le
Gallo, F-92100 Boulogne Billancourt (FR).

(21) Numéro de la demande internationale :

PCT/FR2003/001169

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : AN-
DREAUX, Jean-Pierre [FR/FR]; 20, rue de Lorgeril,
F-35000 Rennes (FR). DIEHL, Eric [FR/FR]; La
Buzardière, F-35340 Liffre (FR). DURAND, Alain
[FR/FR]; 79, rue de Dinan, F-35000 Rennes (FR).

(22) Date de dépôt international : 11 avril 2003 (11.04.2003)

(25) Langue de dépôt :

français

(26) Langue de publication :

français

(74) Mandataire : BERTHIER, Karine; Thomson, 46, quai
Alphonse Le Gallo, F-92648 Boulogne Cedex (FR).

(30) Données relatives à la priorité :

02/04840

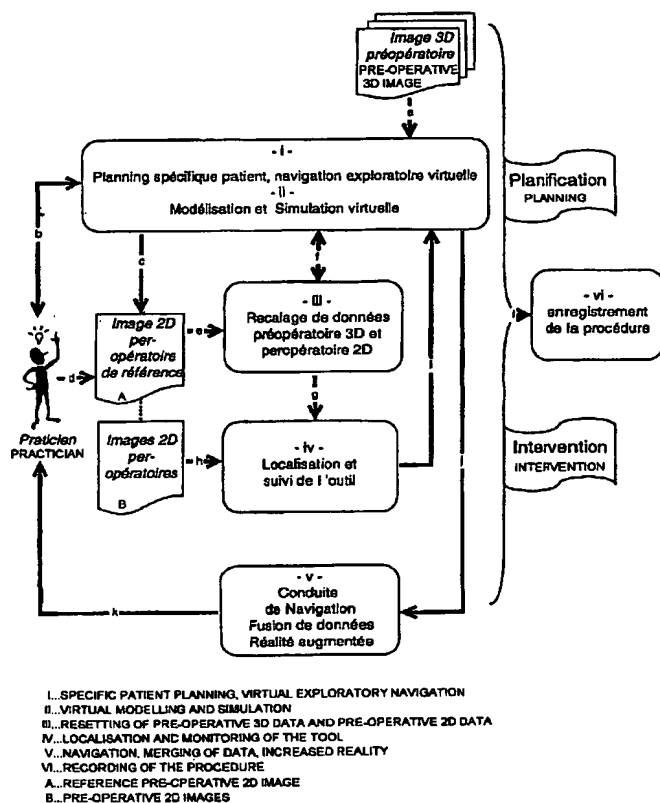
12 avril 2002 (12.04.2002) FR

(81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,

[Suite sur la page suivante]

(54) Title: METHOD FOR THE ANONYMOUS AUTHENTICATION OF A DATA TRANSMITTER

(54) Titre : PROCÉDE D'AUTHENTIFICATION ANONYME D'UN EMETTEUR DE DONNEES



(57) Abstract: The invention relates to a method whereby it can be checked whether data received by a receiver (2) has been sent by a transmitter (1, 3) authorised by a trusted third party, the transmitter and the receiver being connected to a digital network. An identifier (IdEvent) is associated with the data sent by the transmitter and, on receipt of the data by the receiver (2), the receiver generates a random number (C) and diffuses the same on the network. The transmitter that receives said random number calculates a response (R) by applying a first function (G) to the random number (C) and to the identifier (IdEvent), and sends said response (R) to the receiver which verifies the response received by applying a second function (H) to the response received, the random number (C) and the identifier (IdEvent). The first function (G) is delivered first to the transmitter by the trusted third party, and the second function (H) is a function for checking the result of the first function which is delivered first to the receiver by the trusted third party.

(57) Abrégé : Le procédé permet de vérifier que des données reçues par un récepteur (2) ont été envoyées par un émetteur (1, 3) autorisé par un tiers de confiance, l'émetteur et le récepteur étant raccordés à un réseau numérique. Un identifiant (IdEvent) est associé aux données envoyées par l'émetteur et, lorsque les données sont reçues par le récepteur (2), celui-ci génère un nombre aléatoire (C) qu'il diffuse sur le réseau. L'émetteur qui reçoit ce nombre aléatoire calcule une réponse (R) en appliquant une première fonction (G) au nombre aléatoire (C) et à l'identifiant (IdEvent) et envoie cette réponse

[Suite sur la page suivante]



DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés (régional) : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour la désignation suivante US*

- *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour la désignation suivante US*
- *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour la désignation suivante US*
- *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :

— *avec rapport de recherche internationale*

(88) Date de publication du rapport de recherche internationale:

8 avril 2004

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

INTERNATIONAL SEARCH REPORT

Internat

plication No

PCT/FR 03/01169

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L29/06 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MENEZES ET AL: "Handbook of applied cryptography" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US, 1997, pages 400-405, XP002143934 ISBN: 0-8493-8523-7 page 400, line 37, paragraph 10.3.2 - line 40 page 401 -page 405 --- -/-	1-13



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

* & * document member of the same patent family

Date of the actual completion of the international search

1 October 2003

Date of mailing of the international search report

14/10/2003

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2260 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Figiel, B

INTERNATIONAL SEARCH REPORT

terr

lication No

PCT/FR 03/01169

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SCHECHTER S ET AL: "ANONYMOUS AUTHENTICATION OF MEMBERSHIP IN DYNAMIC GROUPS" FINANCIAL CRYPTOGRAPHY. INTERNATIONAL CONFERENCE, XX, XX, 22 February 1999 (1999-02-22), pages 184-195, XP001006339 page 186, paragraph 3 page 187, paragraph 5.1 - paragraph 5.2 -----	1,5
A	US 5 815 665 A (BALAZ RUDOLPH ET AL) 29 September 1998 (1998-09-29) abstract; figure 3 column 2, line 32 -column 3, line 30 -----	1,5

INTERNATIONAL SEARCH REPORT

Serial No.

Application No.

PCT/FR 03/01169

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5815665	A	29-09-1998	NONE

RAPPORT DE RECHERCHE INTERNATIONALE

ionale No

PCT/FR 03/01169

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L29/06 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	<p>MENEZES ET AL: "Handbook of applied cryptography" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US, 1997, pages 400-405, XP002143934 ISBN: 0-8493-8523-7 page 400, ligne 37, alinéa 10.3.2 - ligne 40 page 401 -page 405</p> <p>---</p> <p>-/--</p>	1-13

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

- *A* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- *E* document antérieur, mais publié à la date de dépôt international ou après cette date
- *L* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- *O* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- *P* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

T document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

X document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

Y document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

& document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

1 octobre 2003

Date d'expédition du présent rapport de recherche internationale

14/10/2003

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Figiel, B

RAPPORT DE RECHERCHE INTERNATIONALE

ma

ionale No

PCT/FR 03/01169

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>SCHECHTER S ET AL: "ANONYMOUS AUTHENTICATION OF MEMBERSHIP IN DYNAMIC GROUPS" FINANCIAL CRYPTOGRAPHY. INTERNATIONAL CONFERENCE, XX, XX, 22 février 1999 (1999-02-22), pages 184-195, XP001006339 page 186, alinéa 3 page 187, alinéa 5.1 - alinéa 5.2</p> <p>---</p>	1,5
A	<p>US 5 815 665 A (BALAZ RUDOLPH ET AL) 29 septembre 1998 (1998-09-29) abrégé; figure 3 colonne 2, ligne 32 -colonne 3, ligne 30</p> <p>-----</p>	1,5

RAPPORT DE RECHERCHE INTERNATIONALE

Formai

ionale No

PCT/FR 03/01169

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 5815665	A	29-09-1998	AUCUN